BY ORDER OF THE COMMANDER
AVIANO AIR BASE

AVIANO AIR BASE INSTRUCTION 31-401

17 DECEMBER 2013

Security

INSTALLATION SECURITY ADVISORY GROUP CHARTER

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 31 FW/IP

Certified by: 31 FW/CV
(Col Brent R. Vosseller)

Supersedes: AVIANOABI31-401, 16 October 2012

Pages: 6

This instruction implements SAF/AA *Information Protection Concept of Operations (IP CONOPS) (Attach 2)*, dated 1 Jul 08 and AFI 31-401, *Information Security Program Management*, dated 1 November 2005. It establishes the Installation Security Advisory Group (ISAG) to serve as the single focal point for coordinating information protection efforts within the installation, developing integrated wing level policy, and procedures for information protection. Of note, detailed instructions and policy directives are in development and will be published by SAF when approved. This instruction applies to all organizations on Aviano AB and its geographically separated units (GSUs). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).

SUMMARY OF CHANGES

This document has been substantially revised and must be completely reviewed. This publication is substantially revised and must be read in its entirety. Changes are made on paragraphs 2.1 and 3.1.1.

1. General.

1.1. The ISAG will assist in providing a converged 31 FW enterprise approach to protection of wing information as an integrated group in direct support of the 31 FW mission.

1.2. This is accomplished through a combination of policy development, guidance, and oversight of program execution, IP program processes, and organizational improvements. The group will limit the scope of its proceedings to information protection activities, but will include areas of security outside of information protection as required.

2. Responsibilities.

2.1. The 31 FW/CV is the ISAG Chairman responsible for oversight of program execution and will provide direction/guidance for information protection implementation to the ISAG. Chairman responsibilities can be delegated to 31 MSG/CC, CD or civilian equivalent when the ISAG is combined with the Installation Protection Working Group (IPWG). The 31 FW Chief, Information Protection (CIP) will facilitate and manage all ISAG actions IAW this instruction and higher headquarters instructions/policy guidance (see paragraph 2.2 below).

2.2. The ISAG is a collective, action officer-level forum of security disciplines within the wing whose primary purpose is to develop programs designed to protect the command's information, structures, and networks where information resides. The group is composed of ISAG members and advisors as needed.

2.2.1. **Facilitator.**

2.2.2. 31 FW Chief of IP is the ISAG Facilitator. Responsibilities are to facilitate ISAG meetings and ensure a team lead is appointed for all related sub-ISAG activities.

2.2.3. Schedule meetings, submit agendas for approval to the FW/CV, and notify all ISAG members as appropriate.

2.2.4. Provide leadership and guidance to ISAG members on information protection integration, requirements, programmatic, prioritization, and related issues.

2.2.5. Prepares, coordinates, and maintains requirements according to established guidance and directives as developed for ISAG members.

2.2.6. Establish procedures to include creation, coordination, prioritization, assessment and status reporting as directed by SAF and MAJCOM.

2.2.7. Prepare, coordinate, and present ISAG recommendations.

2.2.8. Assign and manage all ISAG related action items (e.g., assign tracking numbers, Office of Primary Responsibility (OPR) and Office of Collateral Responsiblity, suspense dates). All action items will be forwarded to OPRs and OCRs.

2.2.9. Prepare correspondence (e.g., announcement messages, meeting minutes, collection of briefings, and action items). Minutes will be published following all meetings.

2.2.10. Publish, manage, and archive ISAG related information. Classified information will be maintained within program channels and distributed on as a required basis.

2.2.11. Establish subordinate committees as required.

2.3. ISAG Members.

2.3.1. The ISAG is comprised of subject-matter experts (actions officers) from each of the areas listed below. Ensure appointed members have sufficient authority, expertise to enable expeditious deliberation, collaboration, and implementation of ISAG issues on behalf of their functional directors/commanders. The ISAG is comprised of the following members:

Table 1. ISAG Members

Unit/Organization	Discipline
31 CS	Computer Security (COMPUSEC)
31 CS	Communications Security (COMSEC)
31 CS	Information Assurance (IA)
31 CS	Information Management (FOIA/PII)
31 CS	NATO Subregistry
31 FW/CVN	Advanced Programs
31 FW/IP	Information Security
31 FW/IP	Industrial Security
31 FW/IP	Personnel Security
31 FW/PA	Public Affairs
31 FW/XP	Operations Security (OPSEC)
31 OSS/IN	Sensitive Compartmented Information (SCI)
31 SFS	Integrated Defense

2.3.2. Serve as their organizations primary point of contact.

2.3.3. Empowered to represent and speak on behalf of their organization.

2.3.4. Develop a process to coordinate issues with their organization in an expeditious manner and attempt to reach consensus to resolve issues.

2.3.5. Relate status, impacts, concerns, and recommendations affecting their organization.

2.3.6. Submit and prioritize new information protection requirements to the ISAG.

2.3.7. Review information protection requirements, potential solutions for operational, and technical feasibility.

2.3.8. Validate information protection requirements and approve further processing.

2.3.9. Prepare timely responses to assigned/accepted tasks (action items), and submit to ISAG chair.

2.3.10. Submit proposed agenda and action items to ISAG Facilitator.

2.3.11. Present organization unique, or subject matter expert views, as necessary.

2.4. ISAG **Advisors.** Advisors include, but are not limited to:

Table 2. ISAG Advisors

Unit/Organization	Discipline
AFOSI Det 531	AF Office of Special Investigations
31 FW/IG	Inspector General
31 FW/JA	Legal
USAFE/A5 OL-E (31 FW POLAD)	International Affairs

2.4.1. Serve as their organization primary point of contact.

2.4.2. Review information protection requirements and potential solutions. Voice concerns, make suggestions, and provide comments as appropriate.

2.4.3. Suggest new information protection requirements and solutions for ISAG consideration.

2.4.4. Respond in a timely manner to action items assigned during meetings, and provide a contact name for each action item assigned (OPR/OCR).

2.4.5. Provide subject matter experts to review products and provide input to the ISAG.

3. Procedures.

3.1. The ISAG will meet quarterly or as needed. The ISAG can be incorporated into other like 31 FW working groups or councils.

3.1.1. The ISAG can be combined with the IPWG and meeting minutes will be provided to 31 FW/CV.

3.2. Follow-up.

3.2.1. The facilitator will distribute ISAG action items, meeting minutes to members, and publish meeting information following meetings. Sensitive and classified information will be sent via secure means to members and may be stored on appropriate level systems.

3.3. Subordinate Working Groups.

3.3.1. Meet as necessary and provide periodic, agreed upon updates to the chair before ISAG meetings.

3.4. Designation.

3.4.1. ISAG members (see paragraph 2.3 and 2.4) must be appointed in writing by their unit commander or wing staff agency chief; forward appointment letters to 31 FW/IP. Each appointed member will have a sufficient level of expertise in the designated functional area. Group members must have sufficient authority to deliberate, collaborate, coordinate, and implement ISAG issues on their behalf.

3.5. ISAG Charter Changes.

3.5.1. ISAG or advisory members may suggest policy changes to be addressed at any ISAG meeting. Send proposed changes to the ISAG Facilitator. This charter will be reviewed by the ISAG membership at least every two-years, or as otherwise required. This charter will remain, in effect, until canceled, superseded, or as directed by higher authority.

4. Distribution.

4.1. The 31 FW/IP Chief, Information Protection is my point of contact for this instruction.

JON A. NORMAN, Brigadier General, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 31-401, *Information Security Program Management*, 1 November 2005

SAF/AA *Information Protection Concept of Operations* (IP CONOPS), attachment 2, 1 July 2008

Prescribed Forms

None

Adopted Forms

AF Form 847, Recommendation for Change of Publication

Abbreviations and Acronyms

AFOSI—Air Force Office of Special Investigations

COMPUSEC—Computer Security

COMSEC—Communications Security

FOIA—Freedom of Information Act

GSU—Geographically Separated Units

IP—Information Protection

IPWG—Installation Protection Working Group

ISAG—Installation Security Advisory Group

OCR—Office of Collateral Responsibility

OPSEC—Operations Security

PII—Personal Identifiable Information

POC—Point of Contact

SAF—Secretary of the Air Force

SCI—Sensitive Compartamented Information